

GeekBrains

Урок 2 Видео 1

# Криптография

## Обзор блочных шифров

# В этом видео

1. Устройство блочных шифров
2. AES, Кузнечик
3. pycrypto, OpenSSL

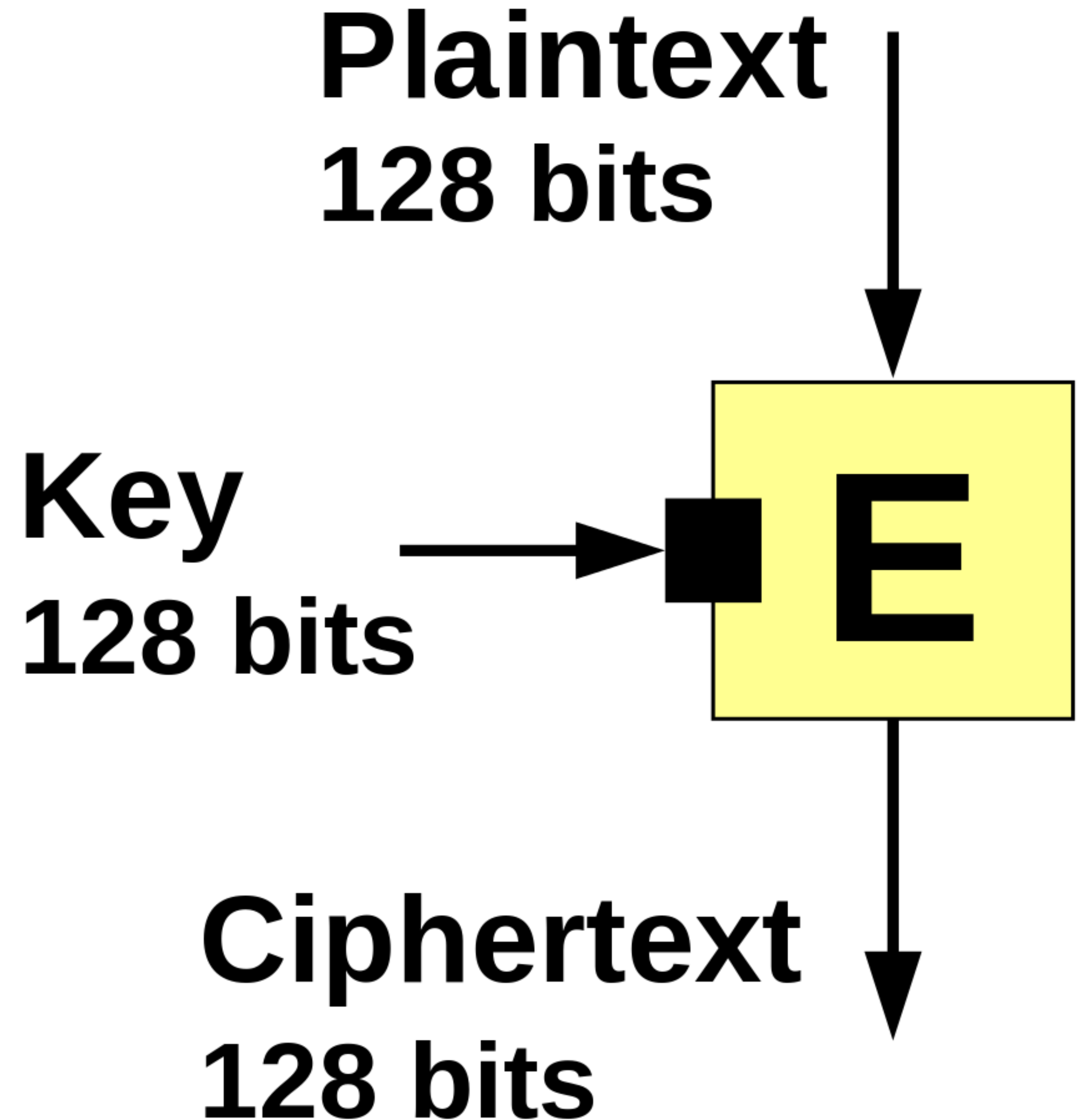
# Как сохранить информацию в тайне?



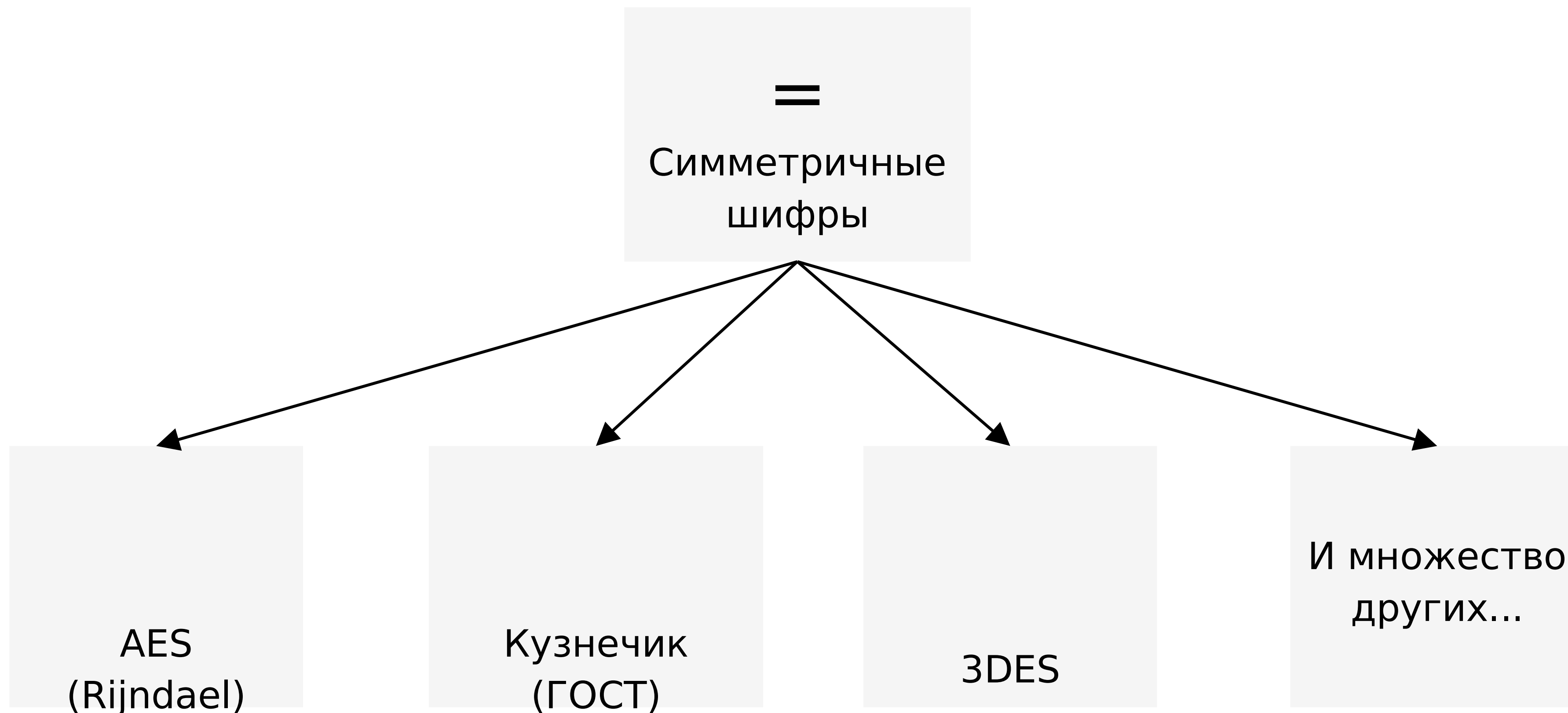
# Блочный шифр

Преобразует открытый текст фиксированного размера в шифротекст фиксированного размера.

Ключ не всегда совпадает с длиной блока.



# Современные симметричные шифры



# Основные характеристики AES и Кузнечика

Размер ключа
AES: 128/192/256 бит
Кузнечик: 256 бит

Размер блока
AES: 128 бит
Кузнечик: 128 бит

# Библиотеки и программы

pycrypto

OpenSSL

# Итоги

1. Узнали верхнеуровневое устройство блочных шифров
2. Характеристики AES, Кузнечик
3. Библиотеки pycrypto, OpenSSL